Docket No.: 22040-00039-US1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto Izawa et al.

Application No.: 10/711,811 | Confirmation No.: 5810

Filed: October 6, 2004 | Art Unit: N/A

For: RANDOM NUMBER INITIAL VALUE GENERATION DEVICE AND METHOD, RANDOM NUMBER INITIAL VALUE GENERATION PROGRAM | Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	2002-134682	May 9, 2002

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00039-US1 from which the undersigned is authorized to draw.

Dated: October 7, 2004
25400_1

Respectfully submitted,

By _____
Larry J. Hume
Registration No.: 44,163
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

10/711,811

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　５月　９日

出願番号
Application Number: 特願２００２－１３４６８２

[ST. 10/C]: [ＪＰ２００２－１３４６８２]

出願人
Applicant(s): 新潟精密株式会社
株式会社マイクロ総合研究所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００４年　９月　１日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

【書類名】　特許願
【整理番号】　14NS1448
【提出日】　平成14年 5月 9日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/14
【発明者】
【住所又は居所】　東京都品川区南品川２丁目２番５号　株式会社マイクロ総合研究所内
【氏名】　井澤　誠
【発明者】
【住所又は居所】　東京都品川区南品川２丁目２番５号　株式会社マイクロ総合研究所内
【氏名】　成田　宏光
【発明者】
【住所又は居所】　埼玉県上尾市緑丘４丁目７番１７号
【氏名】　岡本　明
【特許出願人】
【識別番号】　591220850
【氏名又は名称】　新潟精密株式会社
【特許出願人】
【住所又は居所】　東京都品川区南品川２丁目２番５号
【氏名又は名称】　株式会社マイクロ総合研究所
【代理人】
【識別番号】　100105784
【弁理士】
【氏名又は名称】　橘　和之
【電話番号】　049-249-5122

【手数料の表示】

【予納台帳番号】　070162

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0006161

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　乱数初期値発生装置および方法

【特許請求の範囲】

【請求項１】　ネットワーク上に接続される電子機器において乱数初期値を発生するための装置であって、

上記電子機器の電源が投入されてから、最初に発生したネットワークイベントが上記ネットワークを介して受信されるまでの時間を計測する計時手段と、

上記計時手段により計測された時間情報をもとに上記乱数初期値を決定する乱数初期値決定手段とを備えたことを特徴とする乱数初期値発生装置。

【請求項２】　上記乱数初期値決定手段は、上記計時手段により計測された時間情報に対して所定の演算を行うことにより上記乱数初期値を求める演算手段を含むことを特徴とする請求項１に記載の乱数初期値発生装置。

【請求項３】　上記演算手段により求められた乱数初期値を、上記演算手段が次回の電源投入時に上記乱数初期値の演算に用いるために記憶しておく記憶手段を備えることを特徴とする請求項２に記載の乱数初期値発生装置。

【請求項４】　ネットワーク上に接続される電子機器において乱数初期値を発生するための方法であって、

上記電子機器の電源が投入されてから、最初に発生したネットワークイベントが上記ネットワークを介して受信されるまでの時間を計測し、その時間情報をもとに上記乱数初期値を決定するようにしたことを特徴とする乱数初期値発生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は乱数初期値発生装置および方法に関し、特に、ネットワーク上に接続される電子機器で、キーボードやマウス等の入力デバイスを持たない電子機器の乱数初期値を決定するための装置および方法に用いて好適なものである。

【０００２】

【従来の技術】

第三者の不正な攻撃によりデータが盗聴、改ざん、破壊等されることから守るために、可変パスワードの設定、データの暗号化、電子署名などのセキュリティ技術が用いられる。これらのセキュリティ技術では、ランダムなパスワードや暗号鍵をその都度発生するために、乱数が利用される。乱数を発生するためには、まずは乱数の初期値を決定する必要がある。そして、乱数が真にランダムな値をとるためには、この乱数初期値自体がランダムな値をとることが要求される。

【０００３】

従来、例えばパーソナルコンピュータ（以下、パソコン）において乱数初期値を決める際には、キーボードやマウス等のユーザインタフェースを利用する方法が採られてきた。例えば、ユーザが無作為に所定数のキー入力を行ったり、無作為にマウスを移動させたりすることにより、これらの入力データを用いてランダムな乱数初期値を発生していた。

【０００４】

ところが、このような手法は、キーボードやマウス等のユーザインタフェースが存在しない電子機器では採用することができない。例えば、ネットワーク上に接続されたユーザインタフェースのない電子機器に対して乱数を発生することが必要なシステムの場合には、これ以外の手法を用いる必要がある。

【０００５】

そこで従来は、乱数初期値発生用の専用ＬＳＩを電子機器に搭載する方法や、電子機器が備える揮発性メモリの値を利用して乱数初期値を決定する方法などが採られてきた。揮発性メモリの値を利用する方法は、電子機器の電源が投入されたときに揮発性メモリの値は不定となっているので、その不定値に基づき乱数初期値を発生する方法である。

【０００６】

【発明が解決しようとする課題】

しかしながら、専用ＬＳＩを用いる方法では、その分コストが高くなってしまうという問題があった。一方、揮発性メモリの値を利用する方法では、その値は確かに不定値ではあるが、ランダムな値ではない。そのため、同じような傾向の乱数初期値が発生されることが多く、真にランダムな乱数を発生することができ

ないという問題があった。

【０００７】

本発明は、このような問題を解決するために成されたものであり、ユーザインタフェースを持たない電子機器において、専用ＬＳＩを用いるなどしてコストアップを招くことなく、ランダムな乱数初期値を発生することができるようにすることを目的とする。

【０００８】

【課題を解決するための手段】

本発明の乱数初期値発生装置は、ネットワーク上に接続される電子機器において乱数初期値を発生するための装置であって、上記電子機器の電源が投入されてから、最初に発生したネットワークイベントが上記ネットワークを介して受信されるまでの時間を計測する計時手段と、上記計時手段により計測された時間情報をもとに上記乱数初期値を決定する乱数初期値決定手段とを備えたことを特徴とする。

【０００９】

本発明の他の態様では、上記乱数初期値決定手段は、上記計時手段により計測された時間情報に対して所定の演算を行うことにより上記乱数初期値を求める演算手段を含むことを特徴とする。

また、上記演算手段により求められた乱数初期値を、上記演算手段が次回の電源投入時に上記乱数初期値の演算に用いるために記憶しておく記憶手段を備えるようにしても良い。

【００１０】

また、本発明の乱数初期値発生方法は、ネットワーク上に接続される電子機器において乱数初期値を発生するための方法であって、上記電子機器の電源が投入されてから、最初に発生したネットワークイベントが上記ネットワークを介して受信されるまでの時間を計測し、その時間情報をもとに上記乱数初期値を決定するようにしたことを特徴とする。

【００１１】

【発明の実施の形態】

以下、本発明の一実施形態を図面に基づいて説明する。

図１は、本実施形態の乱数初期値発生装置を適用した電子機器の要部構成例を示すブロック図である。また、図２は、上記図１に示す電子機器を適用したネットワークシステムの全体構成例を示す図である。

【００１２】

図２に示すように、本実施形態の乱数初期値発生装置２ａ，２ｂ，２ｃは、ネットワーク３上に接続された電子機器１ａ，１ｂ，１ｃに各々搭載されている。ネットワーク３上に存在する複数の電子機器１ａ～１ｃは、ルータ４を介して互いにデータの送受信を行うことができるようになっている。

【００１３】

図１に示すように、本実施形態の電子機器１は、乱数初期値発生装置２の他に乱数発生部１４および通信処理部１５を備えている。また、乱数初期値発生装置２は、カウンタ１１、乱数初期値決定部１２およびメモリ１３を備えている。通信処理部１５は、ネットワーク３上に接続されている他の電子機器１との間で、ルータ４を介して互いにデータの送受信を行うための処理を実行する。

【００１４】

カウンタ１１は、電子機器１の電源が投入されたときにカウント値を“０”にリセットしてカウント動作を開始し、最初に発生したネットワークイベントがネットワーク３上から通信処理部１５を介して受信されるまでの時間（例えば、パケットやトークン等の意味のあるデータの他、特別な意味を持たない信号を受信するまでの時間）を計測する。

【００１５】

乱数初期値決定部１２は、カウンタ１１により計測されたカウント値をもとに乱数初期値を決定する。カウント値そのものを乱数初期値として決定しても良いし、カウント値をもとに所定の演算を行うことによって乱数初期値を求めるようにしても良い。この乱数初期値決定部１２は、所定の演算を行う場合にはＣＰＵを備えて構成される。

【００１６】

メモリ１３は、乱数初期値決定部１２により求められた乱数初期値を記憶して

おくものである。このメモリ１３は、例えば不揮発性の記録媒体で構成される。また、メモリ１３を揮発性の記録媒体で構成するとともに、電源がオフとされても記憶内容が消えないように電池等でバックアップしておくようにしても良い。

【００１７】

このメモリ１３に記憶される情報は、乱数初期値決定部１２が次回の電源投入時に新たな乱数初期値を演算するために用いる。すなわち、最初の電源投入時はカウンタ１１により計測されたカウント値をもとに乱数初期値を決定する。２回目以降は、前回の演算によってメモリ１３に記憶された乱数初期値をもとに演算を行い、新たな乱数初期値を求めて再度メモリ１３に格納する。

【００１８】

なお、このようなメモリ１３は設けず、電源が投入される都度、カウンタ１１により計測されるカウント値をもとに乱数初期値を決定するようにしても良い。

【００１９】

乱数発生部１４は、以上のようにして求められた乱数初期値を用いて所定の演算を行うことにより、乱数を発生する。この乱数発生のアルゴリズムについては様々なパターンが考えられ、種々の手法が提供されている。本実施形態では、公知の何れも手法も適用することが可能である。

【００２０】

次に、上記のように構成した本実施形態の乱数初期値発生装置による乱数初期値発生の動作を、図３のフローチャートを参照しながら説明する。

図３において、電子機器１の電源が投入されると、カウンタ１１のカウント値を“０”にリセットした後（ステップＳ１）、カウント動作を開始する（ステップＳ２）。

【００２１】

そして、ネットワーク３上から通信処理部１５を介して最初のネットワークイベント（例えば、パケット等のデータ）が受信されたかどうかを判定する（ステップＳ３）。ネットワークイベントを受信していない場合は、カウンタ１１によるカウント動作を継続し、カウント値をカウントアップしていく。

【００２２】

一方、最初のネットワークイベントを受信した場合は、その時点でカウンタ１１のカウント動作を停止し（ステップＳ４）、そのときのカウント値をもとに乱数初期値決定部１２により乱数初期値を決定する（ステップＳ５）。

【００２３】

以上詳しく説明したように、本実施形態では、電子機器１の電源オンから最初のイベント受信までの時間が一定でなく、ランダムとなることを利用して乱数初期値を決定している。これにより、キーボードやマウス等のユーザインタフェースのない電子機器においても、専用ＬＳＩを用いるなどしてコストアップを招くことなく、ランダムな乱数初期値を発生することができるようになる。すなわち、カウンタ１１や乱数初期値決定部１２のＣＰＵは電子機器１に一般的に備えられているものであるから、既存のハードウェア構成を利用してランダムな乱数初期値を発生することができる。

【００２４】

本実施形態の乱数初期値発生装置は、様々なシステムに適用することが可能である。例えば、可変のパスワードや暗号鍵などを発生するために乱数を利用するネットワーク上の電子機器に適用することが可能である。なお、ネットワーク上に接続された外部サーバなどにより電子機器の乱数初期値を設定することも可能であるが、暗号化通信を始める前の乱数初期値の通信が平文で行われるため、これが盗聴されて暗号鍵を解読される可能性が高くなる。これに対して本実施形態では、乱数初期値発生装置を搭載した電子機器が内部で乱数初期値を自己発生するので、乱数初期値が盗聴される危険性は殆どなく、暗号化通信の安全性を高めることができる。

【００２５】

また、本実施形態の乱数初期値発生装置は、ネットワーク上に接続された複数のスレーブ機器のアドレスをマスタ機器において設定するようなシステムにも適用することが可能である。例えば、マスタとなるＤＳＵ（Digital Service Unit）がスレーブとなる複数のＴＡ（Terminal Adapter）に対して異なるアドレスを設定する際には、各ＴＡがランダムな値を発生してＤＳＵに申告する必要がある。その際に、それぞれのＴＡに対して本実施形態の乱数初期値発生装置を適用す

ることが可能である。

【００２６】

ＤＳＵとＴＡとの通信の場合、複数のＴＡがたとえ同じアドレスを申告しても、そのことをＤＳＵからＴＡにフィードバックして再度申告をやり直すことにより、最終的には全てのＴＡに異なるアドレスを設定することが可能である。しかし、従来のように揮発性メモリの値を用いて乱数初期値を発生すると、複数のＴＡが同じアドレスを申告する可能性が高くなり、申告を何度も繰り返し行う必要が生じる。これに対して本実施形態によれば、一度の申告で複数のＴＡに異なるアドレスを設定できる確率が高まり、電源オンからシステムが動き出すまでの時間を短縮することができる。

【００２７】

なお、以上に説明した実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００２８】

【発明の効果】

本発明は上述したように、電子機器の電源が投入されてから、最初に発生したネットワークイベントが受信されるまでの時間を計測し、その時間情報をもとに乱数初期値を決定するようにしたので、ユーザインタフェースを持たない電子機器において、専用ＬＳＩを用いるなどしてコストアップを招くことなく、ランダムな乱数初期値を発生することができる。

【図面の簡単な説明】

【図１】

本実施形態の乱数初期値発生装置を適用した電子機器の要部構成例を示すブロック図である。

【図２】

図１に示す電子機器を適用したネットワークシステムの全体構成例を示す図である。

【図３】

本実施形態による乱数初期値発生動作を示すフローチャートである。

【符号の説明】

１　電子機器

２　乱数初期値発生装置

３　ネットワーク

４　ルータ

１１　カウンタ

１２　乱数初期値決定部

１３　メモリ

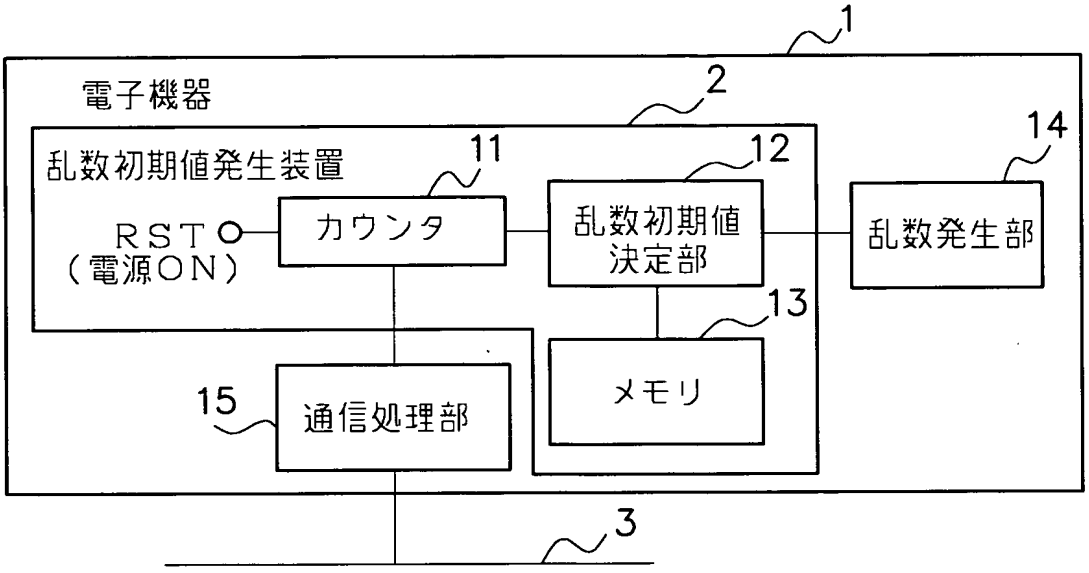
１４　乱数発生部

１５　通信処理部

【書類名】　図面

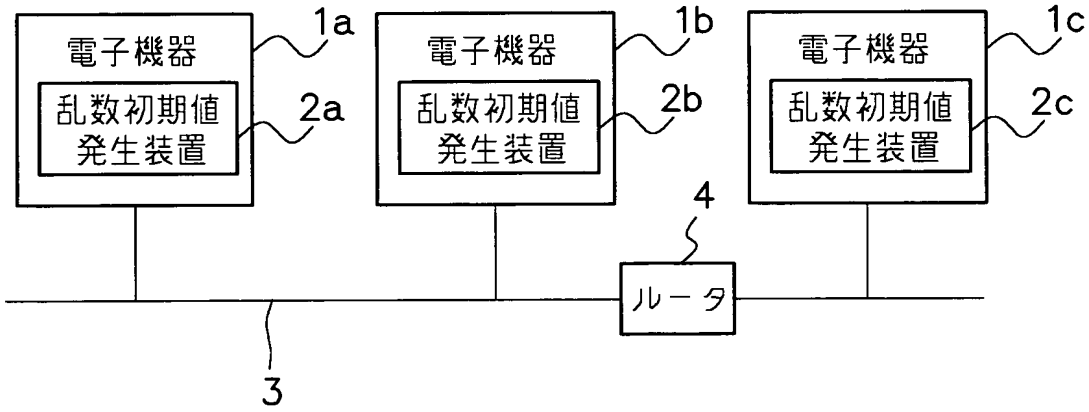
【図１】

本実施形態の乱数初期値発生装置



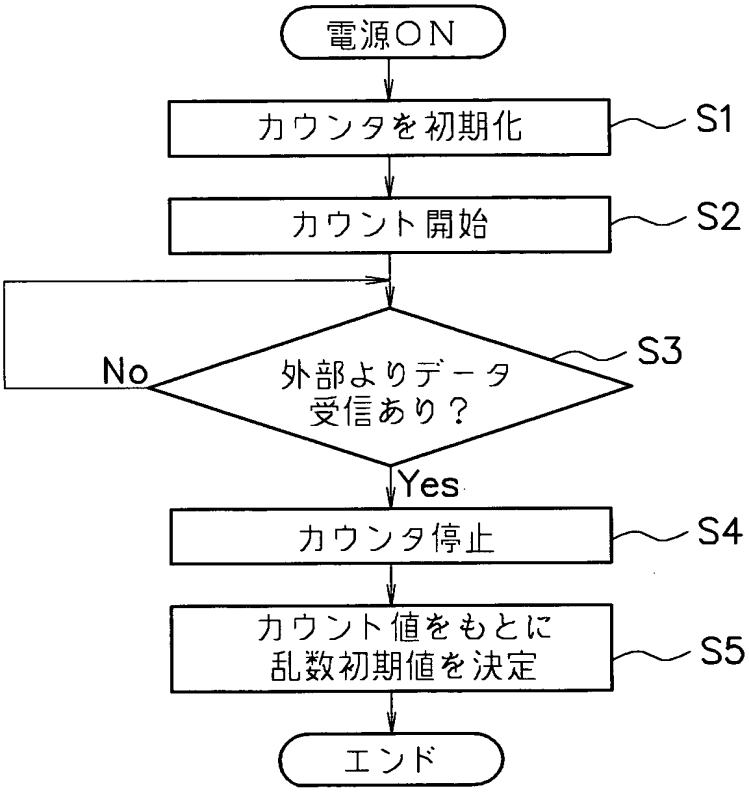
【図２】

本実施形態のネットワークシステム



【図３】

本実施形態による乱数初期値発生動作



【書類名】　　要約書

【要約】

【課題】　専用ＬＳＩを用いるなどしてコストアップを招くことなく、ランダムな乱数初期値を発生することができるようにする。

【解決手段】　電子機器１の電源が投入されてから、最初に発生したネットワークイベントがネットワーク３を介して受信されるまでの時間を計測するカウンタ１１と、カウンタ１１により計測された時間情報をもとに乱数初期値を決定する乱数初期値決定部１２とを設けることにより、カウンタ１１や乱数初期値決定部１２のＣＰＵなど電子機器１に一般的に備えられている既存のハードウェア構成を用いて、電子機器１の電源オンから最初のイベント受信までの時間が一定でないことを利用してランダムな乱数初期値を発生することができるようにする。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００２－１３４６８２
受付番号	５０２００６６７５５２
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年　６月２８日

＜認定情報・付加情報＞

【手数料の表示】

【納付金額】　　12,400円

次頁無

特願２００２－１３４６８２

出　願　人　履　歴　情　報

識別番号　　［５９１２２０８５０］

１．変更年月日　　１９９６年　５月　９日
［変更理由］　　住所変更
住　所　　新潟県上越市西城町２丁目５番１３号
氏　名　　新潟精密株式会社

特願２００２－１３４６８２

出　願　人　履　歴　情　報

識別番号　［５０１３０６９７７］

１．変更年月日　２００１年　８月　２日
［変更理由］　新規登録
住　所　東京都品川区南品川２丁目２番５号
氏　名　株式会社マイクロ総合研究所